

Decode Cyber

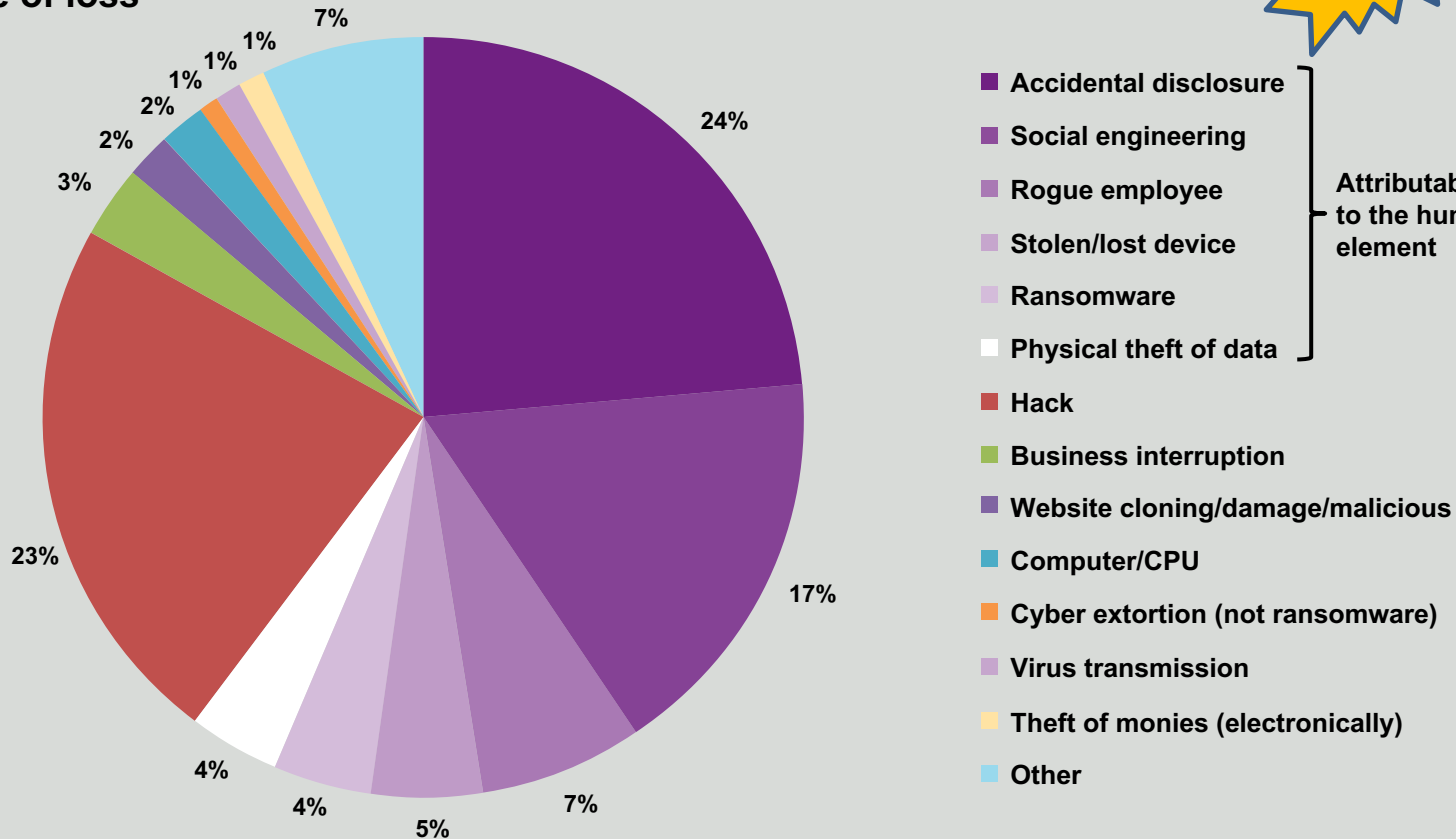
Building an Effective Cyber Risk Culture

Association of Corporate Counsel
2019 Annual In-House Symposium
April 26, 2019

CLG Proprietary Cyber Claims Data

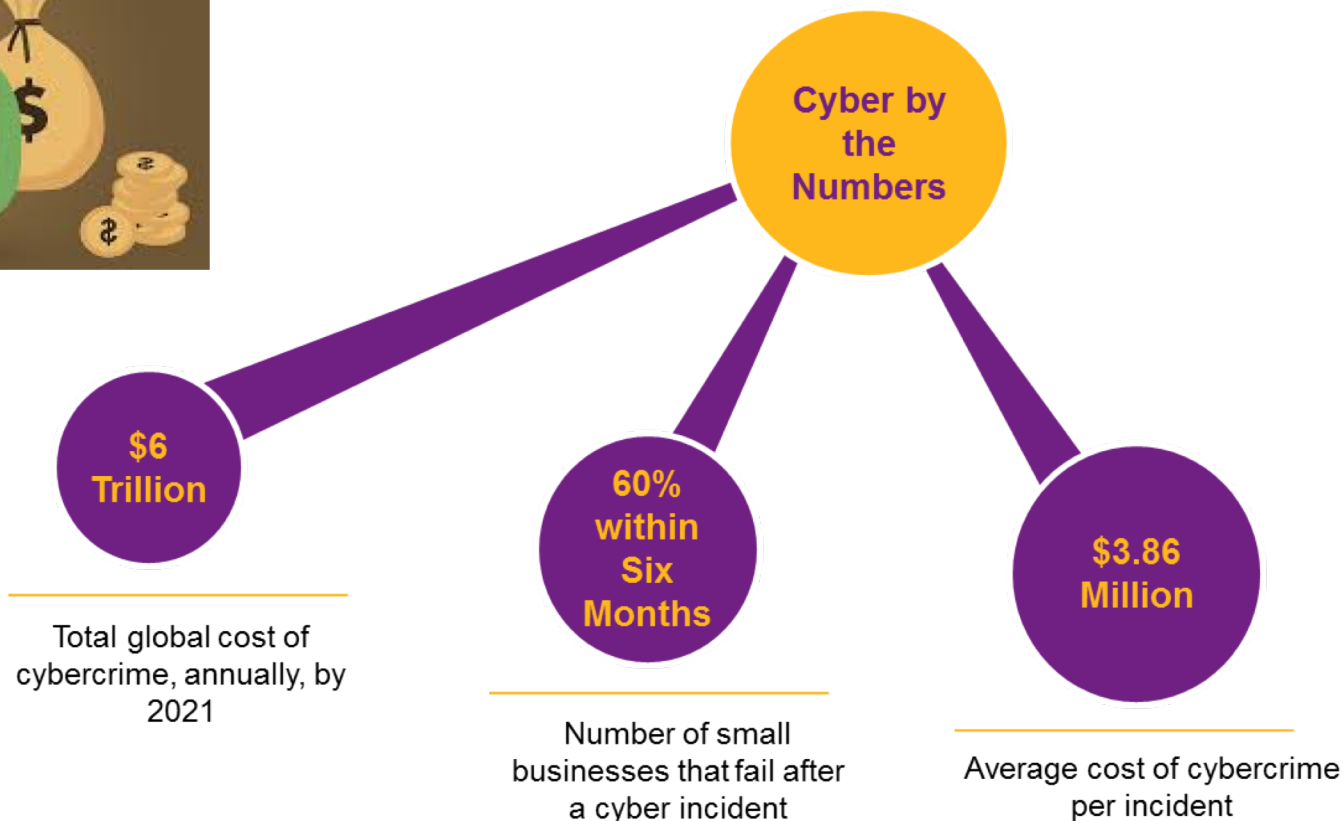
2017-2018 Reported claims index

Type of loss



Willis Towers Watson 2017-18 Reported Cyber Claims Index

Cybercrime and the Cybersecurity Dynamic



Sources: Cybercrime Damages \$6 Trillion by 2021 – <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>; Cyber Threat is Huge for Small Businesses -- <https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/>; The Total Cost of a Data Breach – Including Lost Business – Keeps Growing -- <https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826>

People-Based Cybersecurity Solutions

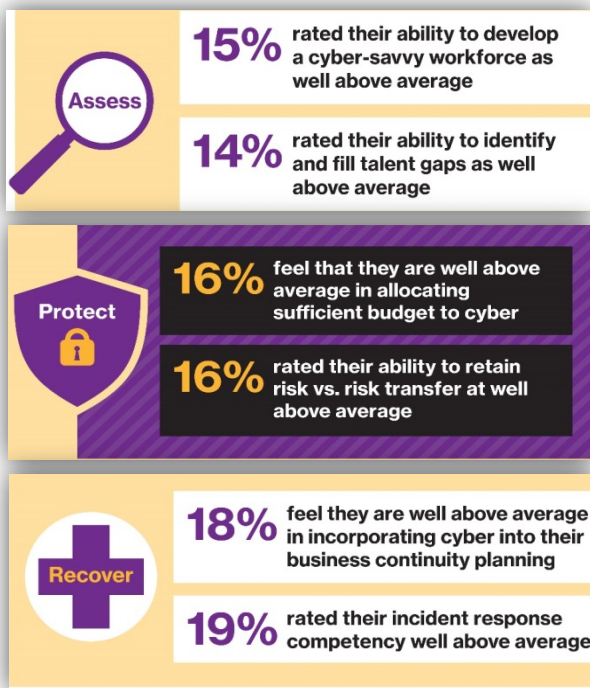
The stark reality

Serious cyber incidents



1/3
of companies surveyed reported one

Most place high odds it will happen again in 12 months



Vulnerabilities exist

Workforce resiliency needs much improvement.

Executives who rate their cyber-resilience competencies well above average

13% Applying lessons learned (worst self-assessment)

21% Integrating technology and governance post-acquisition

15% Ability to develop a cyber-savvy workforce

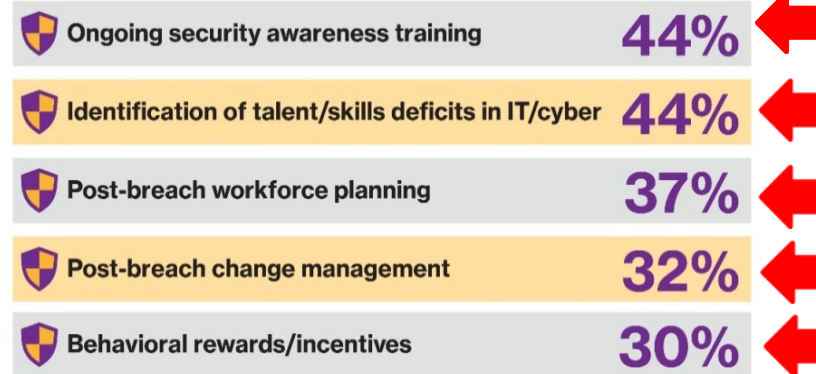
14% Ability to identify and fill talent gaps

Mitigating the human element of cyber risk

Less than half of the companies surveyed have implemented basic cyber-related HR policies.



Policies employed:



Source: How boards can lead the cyber-resilient organization – http://intranet.willistowerswatson.com/wtwIntranetLibrary/EIU_Report_Cyber_Resiliency_FINAL.pdf

People-Based Cybersecurity Solutions

How organisations are allocating their budget

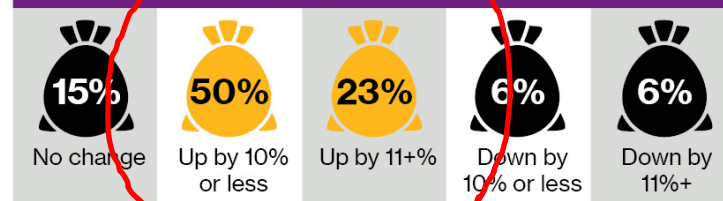
Average spend on cyber-resilience is **1.7% of revenue. Approximately 1/3:**



There's room for improvement

Executives don't believe their companies are spending enough on cyber-resilience.

What investments should look like:



Future spend - **50%** will be allocated to mitigating the human element

How executives think that investments should be deployed:

| | |
|--|-----|
| Technology | 20% |
| IT talent acquisition, skills training/development | 19% |
| Business continuity and disaster recovery | 16% |
| Rewards and incentives | 16% |
| Training | 15% |
| Insurance | 14% |

A disruptive approach

Technology is necessary - but not sufficient alone and certainly no longer the differentiator it once was. As the emphasis shifts from cyber-security to cyber-resilience, business, processes and workforce considerations are becoming more important relative to specialised technical expertise.



Source: How boards can lead the cyber-resilient organization – http://intranet.willistowerswatson.com/wtwIntranetLibrary/EIU_Report_Cyber_Resiliency_FINAL.pdf

Where Should Companies Spend on Cyber Risk Culture?



Cybersecurity Superheroes

Chief Human Resources
Officers

Chief Information Security
Officers

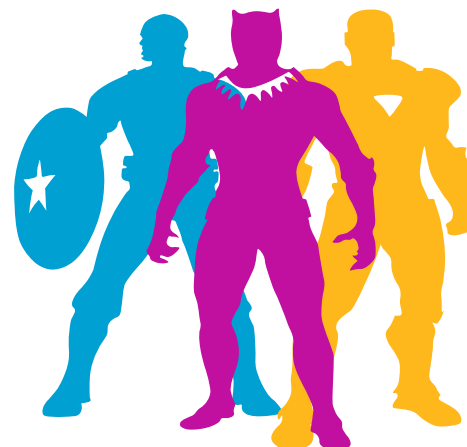
Chief Risk
Officers



Three Musketeers

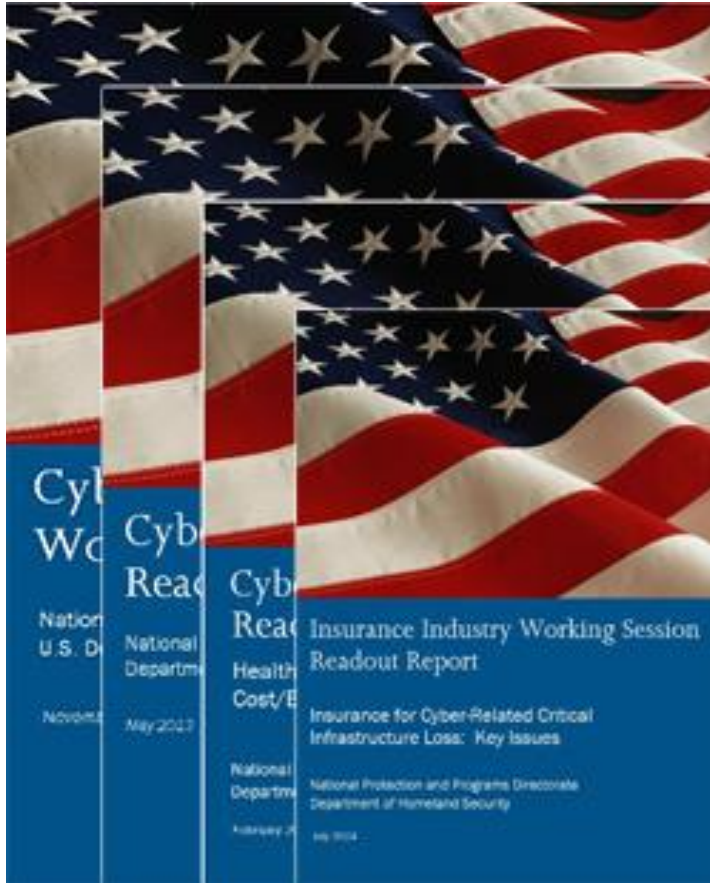


Luke, Leia, and Han



**Captain America,
Black Panther, and Iron Man**

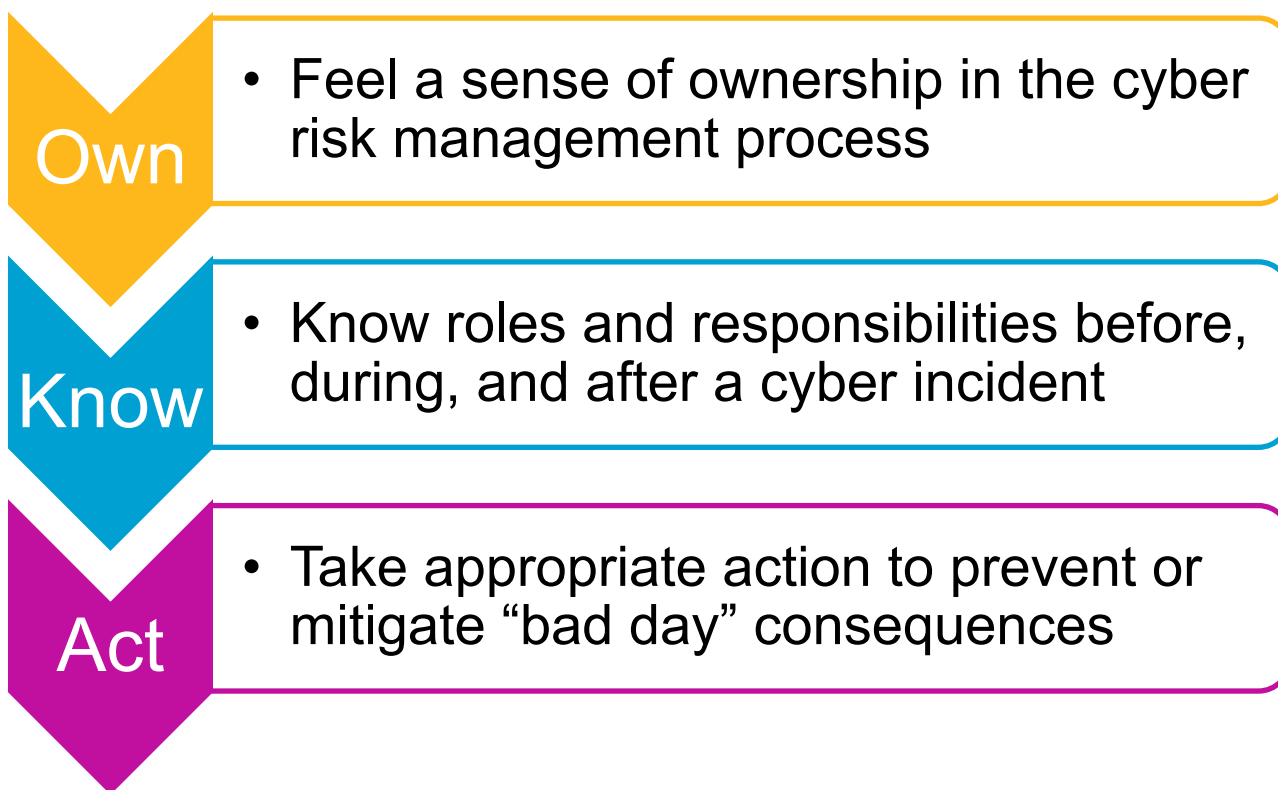
U.S. Department of Homeland Security



- How can we promote a more robust cybersecurity insurance market?
- Fire insurance market as model
- Risk management experts:
 - Insurance brokers and underwriters
 - Corporate risk managers
 - CISOs and CIOs
 - Social scientists
 - Critical infrastructure owners and operators
- **Risk culture is everything**

Defining Terms

An effective cyber risk culture is one where all employees:



The Four Pillars



Pillar I: Engaged Executive Leadership



Tone at the
Top



Karate Kid
and ERM



Sticks and
Carrots

Pillar II: Relevant Training and Awareness



Pillar III: Governance and Process



Pillar IV: Cybersecurity Workforce Strategy



War for
Talent



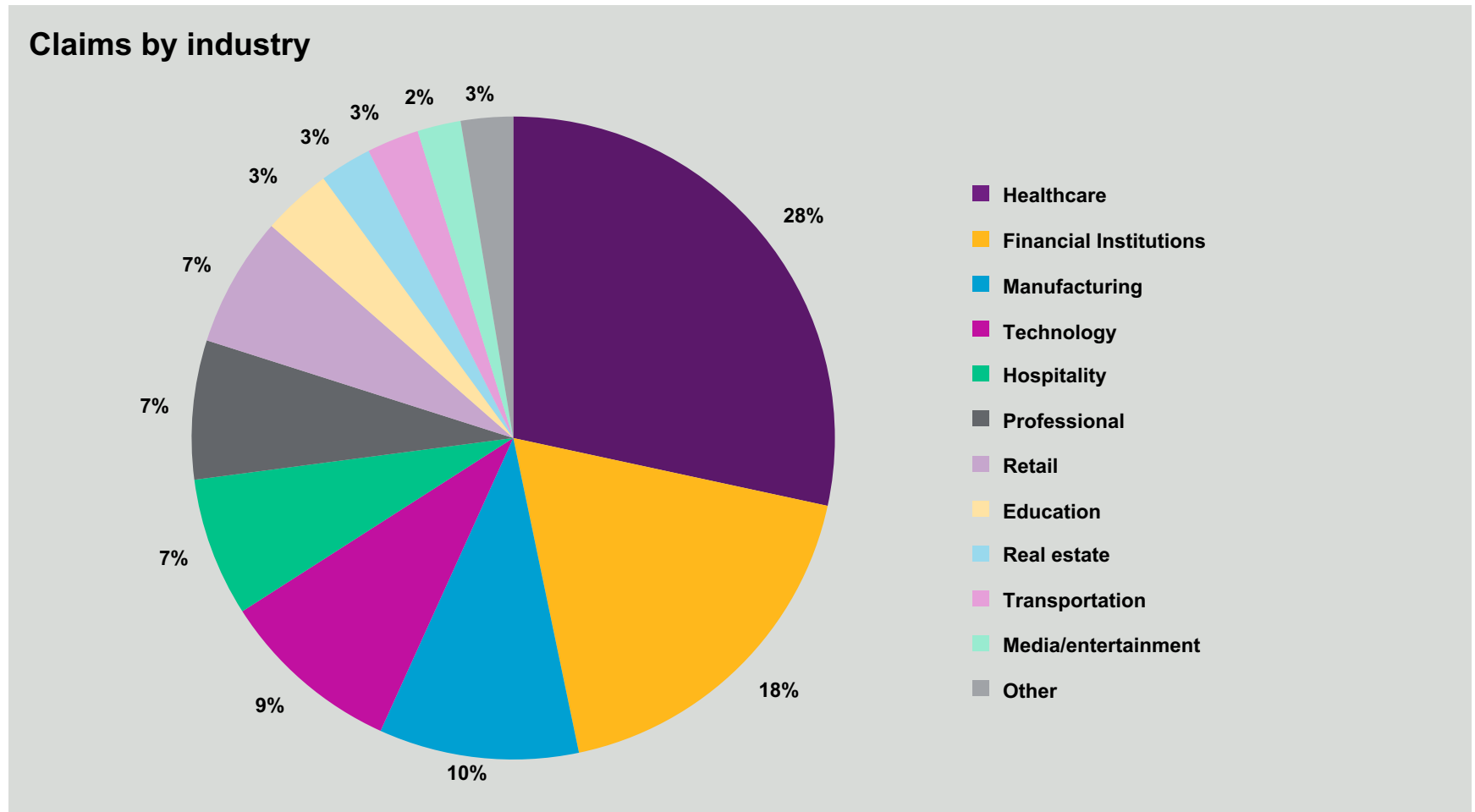
Shaving My
Head








I Want You

CLG Proprietary Cyber Claims Data

2017-2018 Reported Claims Index



State of the Cyber Insurance Market 2018 – Q4

|  Capacity Scattered |  Coverage Careful Expansion |  Claims & losses Rising |  Premiums & retentions Normalizing |  Markets Unaligned |
|---|--|--|--|--|
| <ul style="list-style-type: none"> With well over 60 markets offering some form of cyber /E&O coverage, there is nearly \$1B of capacity available in the marketplace Primary and excess capacity continues to expand and is available domestically, through London, Bermuda and additional international markets New capital and capacity continue to flow into the marketplace, providing insurance buyers with more options Notwithstanding these new entrants, recent claim activity has affected a small subset of carriers who are reducing their capacity and appetite on both primary and excess layers | <ul style="list-style-type: none"> Markets are offering expanded wrongful collection and voluntary shutdown coverage largely in response to increased regulations Non regulatory related expansions include coverage for Forensic Accountants, Reputational Damage coverage and reinstatement of limits provisions in certain industries Reputational Damage coverage has had limited success based on the long periods of indemnity, additional premium and sub-limits Cyber product offerings still vary widely and there is no uniform set of coverage terms, exclusions, definitions, or conditions While coverage continues to broaden across the marketplace, manuscripting coverage is necessary to ensure coverage responds to client exposures | <ul style="list-style-type: none"> According to the 2018 Cyber Risk Outlook, prepared by the University of Cambridge, cyber risk is becoming increasingly international. Cyber losses are being reported in almost every country of the industrialized world according to the RMS Cyber Loss Experience Database, a compilation of all known hacks, attacks, accidents and malware occurring to public and private sector organizations The human element continues to be the leading cause of cyber risk, representing 61% of the claims included in WTW 2017-18 Reported Claims Index Insurers' are starting to see at least 2-3 business interruption claims a year with losses exceeding the waiting period The costs associated with managing cyber and privacy claims, including forensic investigations and defending regulatory actions with associated fines, are on the rise | <ul style="list-style-type: none"> Retentions at all levels are available, but can vary greatly based on industry class, size of organization and particular exposures Insurers' have tightened pricing and retention guidelines for companies that have not addressed vulnerabilities While the market remains competitive, carriers are beginning to push back on price decreases and expanded terms, especially with regard to business interruption coverages Renewal pricing ranges from flat to 15% increases depending on the security controls and privacy protections in place and type of service provided | <ul style="list-style-type: none"> Although we have not yet seen the widespread adoption of big data/AI tools to supplement underwriting, the expectation is that this will be leveraged more in the coming years Carriers continue to push for in depth underwriter meetings, paying particular attention to human capital practices, corporate structure and reporting practices Markets have waived standard applications for select large organizations with mature risk management programs Insurers' continue to innovate and build out their pre-breach and post-breach response services There is still considerable uncertainty surrounding expanding global regulation such as the GDPR and the upcoming CA Privacy Act and the potential for increased regulatory action claims and associated non-compliance fines/penalties. |

Conclusion

